Nr

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/120,763	07/22/1998	MARK H. ETZEL	29250-000262/US	2566

30593 7590 04/06/2004

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
SEAL, JAMES	
ART UNIT	**PAPER NUMBER**
2135	25

DATE MAILED: 04/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/120,763	ETZEL ET AL.
	Examiner	Art Unit
	James Seal	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 27 January 2004.

2. Terminal disclaimers dated 30 December 2003 have been entered.

3. Amendment to the specification have been entered.

4. Claims 1-18 are pending.

Specification

5. With amendment to the specification, the examiner withdraws his objection.

Double Patenting

6. With the receipt and entry of the terminal disclaimers, rejection on grounds of obviousness-type double patenting is withdrawn.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1 -5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds (EP 0532228 A2) and further in view of Laufer (Discrete Mathematics and Applied Modern Algebra).

9. As per claim 1, an enhancement for the CMEA (Cellular Message Encryption Algorithm) for a wireless telephone recites the limitation of an input message (Reed, Figure 9, element 502), the limitation of a first encryption transformation (Reed, Figure element 505), the limitation of using a involution transformation Column 11 lines 1-25 and figure 9, element 507) and the application of a k = TBOX[q], followed by a final transformation (Figure 9, element 511), which yields an output 504.

10. The limitation of the use of one or more offsets is disclosed by Reed in the use of autokeyed encryption (see for example the 5 line of the abstract) in which the key is derived from a portion of the message. Autokeying as is well known in the art requires an offset, that is the ith message is encrypted by the i+k th character of text where k ≥ 1 and is called the offset. Reed is silent on the limitation of iteration the involution operation in the second stage and unlike the first and third stages this would not provide much in the way of diffusion of the key material into the cipher. One of ordinary skill in the art seeking to strengthen the security of the algorithm would have been motivated to provide an iterative cipher for the same reason that DES, IDEA, FEAL and other successful cipher use iteration, to ensure diffusion of the key material throughout the ciphertext. It should be noted by way of contrast that autokeying already provides a diffusion of the key material throughtout the ciphertext.

11. Reeds further discloses a three stage encryptor (see Figure 9) and according to one embodiment, the first stage consist of autokeyed encryptor (that is, the key is derived from a portion of the message as encrypted by the encryptor, Column 3, lines 13-15), the second stage uses a one time pad encryption (that is a Vernam cipher, see Abstract line 5) composed of iterative (see Column 9, lines 45-67, consisting of initializing and updating values as the values are iterated over the integers z) self-

inverting (involutions) which are implemented by an array TBOX[z] = z and a third stage is a second autokeying decryption that corresponds to the autokeyed encryption of the first stage (i.e., the inverse of the first stage, Column 9, lines 61-62), using an 8-bit microcomputer (Abstract, Column 3, lines 6-16; Columns 9, lines 13-20, lines 43, 49-50; Column 11, lines 5-12). As discussed above, autokeying requires at least one offset, between the plaintext and the autokeyed text and thus Reeds must have at least two offsets, one for each autokeyed transformation. Multiloop autokeying would require several offsets (one for each loop). Reeds calculation are performed with an 8-bit microprocessor and thus the cryptographic functions are *discrete functions* (Column 3, line 9), that is their inputs and output are over a discrete set of integers. Reeds is silent on the use of table lookup to evaluate involutions although he does refer to the TBOX[z] as an array. Reed is silent on the inputs to the enhanced TBOX function being subjected to a permutation. With regards to permutations being applied as input to the TBOX, it is well known in the art that permutations are used to eliminate the characteristic footprint of the encryption algorithm. DES using permutations with the iterative encryption algorithm together with the key scheduling. For this reason one of ordinary skill in the art at the time the invention was made would have been motivated to encorporate permutations because they help remove the characteristic signature (footprint) of the algorithm and thus making it more difficult for a cryptanalysis to find an entrance into the cipher.

12. Finally Reed is silent with regards to the use of involuntary lookup. The implementation of iterative algorithmic function such as involutions is often resource intensive. Laufer (Discrete Mathematics and Applied Modern Algebra) teaches the use of tables pages 209-211) such discrete and in particular the discrete involution function page 210, viii. One of ordinary skill in the art at the time the invention was made would

have been motivated to combine the teachings of Reed using involutions for encryption with the table lookup because use of lookup is less resource intensive which is exactly what is needed for cellular phones, which have limited resources. Claim 1 is rejected.

13. As per claim 2, the further limitations that there are one or more secret offsets is disclosed by Reeds in that Reeds autokeys each transformations of the transformation. In fact if one considers multi-looped autokeying there is an offset for each loop. Claim 2 is rejected.

14. As per claim 3, the further limitations that the step of generating the first and second offset is accomplished by combining an external value with one of a plurality of secret values.

15. Reeds discloses that the offsets depend on time (an external value, Column 10, lines 6-7) and secret values e.g. from the SSD-B subfields (lines 17-18). Claim 3 is rejected.

16. As per claims 4 and 5, the further limitation that the secret value includes two 8-bit values for each offset and further the external value is 8-bit value.

17. Reeds discloses that the calculations are to be performed on an eight-bit processor. Claims 3 and 4 are rejected.

18. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds and Laufer as applied to claims 1 and 5 above, and further in view of Vernam (Cipher Printing Telegraph System).

19. As per claim 6, the further limitation that the two offsets are to be calculated from the external value CS_n and the two secret values K_0 and K_1 as follows: offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$ and offset 2 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$.

20. If one considers Reeds' second embodiment, that is, using a secret values (i.e. from the SSD-B subfield) and an external value (say corresponding to the time, Column 10, lines 6-7), to generate the two autokey offset (or a pularity of such offsets for multiloop autokeying), iterating a one time pad (a Vernam cipher AIEE, Feb 1926, pages 109 –115, in particular *Running key ciphers*, page 113, lines 21-24. Reeds differs from claim 6 in that details of Vernam's one time pad are not provided. As applied to the calculation of an offset, Reeds' two secret values K1 and K2 appear as keys and the external value appears as the quantity to be encrypted. A product of the second key with the external value (to prevent frequency cryptananalysis, page 112 column 2) is then XORed (i.e., $\oplus$) by the second key (see page 113, second column 2 lines 22-25). However, to make the key as long as possible without repetition, Vernam used two key tapes which were set up such that a complete circuit around the first tape would advanced the second tape by 1 (pages 133, and 114 both second column). Mathematically one can represent what Vernam did mechanically using paper tapes, by a modular product of the second secret value by the external value mod n and mod (n+1). The first moduli applies to the first tape and the second moduli applies to the second type and the differ in moduli to insure that one circuit around the second loop does not cause a repetition before the first loop is finished. Thus Reeds' two secret

offsets are calculated in the same way as ciphertext in a one time pad. As Reeds' uses 8-bit cryptoprocessor the range of values of 0 to 256 (see Column 10, line 43) i.e., n = 256 (above) for the "tapes". The offset Reeds/Vernam differs from that recited in that K_2 is replaced by $K_2 + 1$, where K_2 is the second secret value. However, the examiner takes official notice that in order for the autocoder to function the offset must always be one or more. To insure this happens, we would then add one to the second secret value. As Reeds does not provide the details of a one time pad, thus one of ordinary skill in the art would have been motivated to review the teachings of Vernam to obtain the details of the one time pad. Claim 6 is rejected.

21. Claims 7- 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, Laufer and Vernam as applied to claims 1 and 6 above, and further in view of Takaragi et. al. (5,222,139).

22. As per claims 7 and 8, the limitation first and second transformation respectively includes bit trading and involution lookup with feedback, random byte permutation, feedback employing both the first and second secret offsets.

23. Reeds disclose the a multistage encryption system that uses discrete involution and Laufer provides table look up to evaluate discrete functions, and feedback (see figure 5b), but are silent on specific involution transformations. Reeds does not disclose the specific types involutions. Takaragi et. al. teach the use of other discrete involutions such as bit trading (bit swapping), bit rotation, bit and bit shifting bits left or As Reeds does not provide the details of particular involutions, one of ordinary skill in the art would have been motivated to review the involutions as applied to bit streams. Claim 7 and 8 are rejected.

24. Claims 9-16 recite the corresponding decryption system to complement the encryption system recited in claims 1-8. Decryption is an essential part of a cryptosystem and as noted above the prior art discloses an encryption/decryption systems. Claim 9-16 are rejected.

25. Claim 17 recites an apparatus (a secure wireless headset or secure cellular phone) with transceiver, input/output interface, key generator for generating one or more keys and a cryptoprocessor, with an input/output interface a message to be encrypted or decrypted together with a message ID's. This is standard in any cell phone and is included in the prior art cited above. The claim recites the CMEA process , with one or more offsets, tbox, employing involutions lookup, were already addressed in claim 1. Claim 17 is rejected.

26. Claim 18 recites a wireless base station consisting of a transceiver, input/output interface, key generator for generating one or more keys, a cryptoprocessor for encryption/decryption of messages together with message ID's. . This is standard in any base station administering to cell phones and is included in the prior art cited above. Further the claim recites a reverse enhanced CMEA processor including a first and second inverse transformation, tbox, offsets, involution lookup. These limitations have been addressed in claim 9. Claim 18 rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

Applicant's arguments filed 27 January 2004 have been fully considered but they are not persuasive. In particular the applicant has suggests that Reed makes no use of offsets. In the Abstract and Column 11, lines 39-42, Reed mentions the use of autokeying. Autokeying ciphers require one or more offsets depending on how many

loops are used. Further features such as feedback must be used in autokeying. Further autokeying are used in any one-time pad ciphers as for example the type first purposed by Vernam. Vernam use multilooped tapes (see figure 1) to modularly add in a "random stream" into his stream cipher. Each such loop requires an offset. The use of iteration of a cipher algorithm is consider good practice as pointed out by Feistel (Cryptography and Computer Privacy). Iterative algorithms provide better confusion and diffusion of the key material. This means that a cryptanalysis can not analyze the ciphertext in depth as each ciphertext character is the results of all keying material and not just of a few. This philosophy has been brought forth in all modern ciphers such as DES, IDEA, FEAL and AES. Further the addition of permutations tend to erase the signature of a particular cipher algorithm thus denying a cryptanalysis a entrance into the cipher. Laufer was used only in connection with the teaching of involutary table lookups.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JWS

Jws
AU 2135
4 April 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100